UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,846	12/21/2001	Keith Alexander Harrison	30003039-2	5756

7590 09/16/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
BERGER, AUBREY H	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 09/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/023,846	HARRISON ET AL.	
	Examiner	Art Unit	
	Aubrey H. Berger	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☒ Claim(s) *1 and 36-40* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *21 December 2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-41 are pending.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 12/21/2001 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Specification

4. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

5. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: "Communication and authentication of a composite credential utilizing obfuscation".

6. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or
REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

7. The abstract of the disclosure is objected to because

a. "authorisation" is misspelled on page 2, line 17;

b. "minimise" is misspelled on page 3, line 12;

c. "unauthorised" is misspelled on page 4, line 25;

d. "forth enterprise 38" on page 7, line 2 should be replaced with "fifth enterprise 38";

e. "fifth enterprise 40" on page 7, line 3 should be replaced with "sixth enterprise 40";

f. "Internation" on page 9, line 16 should be replaced with "International";

g. "organisation" on page 10, line 1 is misspelled;

h. "recognised" on page 10, line 30 is misspelled.

i. Correction is required. See MPEP § 608.01(b).

Claim Objections

8. Claims 1 and 36-40 objected to because of the following informalities:

j. Regarding claims 1 and 36-40 each element or step of the claim should be separated by a line indentation. See MPEP § 1.75 (i).

Appropriate correction is required.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 1-21 and 36-40 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

k. Claim 1, line 6, "which" is unclear and should be replaced with "wherein said";

l. Claim 11, line 2, recites "a composite credential", it is unclear whether this is the same as "the composite credential" as recited to in claim 8.

m. Claim 11, line 2, recites "a plurality of credentials", it is unclear whether this is the same as "a plurality of credentials" as recited in claim 6.

n. Claim 11, line 3, recites "variably obfuscated" and is unclear and is understood as the plurality of credentials are obfuscated.

o. Claim 13, line 2, recites "a first party", it is unclear whether this is the same as "a first party" in claim 1.

p. Claim 13, line 2, recites "a second party", it is unclear whether this is the same as "a second party" in claim 1.

q. Claim 13, line 30, "which" is unclear and should be replaced with "wherein the".

r. Claim 16, line 3, "which" is unclear and should be replaced with "wherein the".

s. Claim 36, line 4, "which" is unclear and should be replaced with "wherein the".

t. Claim 37, line 4, "which" is unclear and should be replaced with "wherein the".

u. Claim 38, line 34, "which" is unclear and should be replaced with "wherein the".

v. Claim 38, lines 5-7 recite "in which composite credential a plurality of credentials is variably encrypted" is unclear and is understood to mean "in which the composite credential comprises a plurality of credentials, wherein each credential is individually encrypted".

w. Claim 39, line 4, "which" is unclear and should be replaced with "wherein the".

x. Claim 40 recites the limitation "the first party" in line 2. There is insufficient antecedent basis for this limitation in the claim and is understood to mean "a first party".

y. Claim 40 recites the limitation "the second party" in 2-3. There is insufficient antecedent basis for this limitation in the claim and is understood to mean "a second party".

z. Claim 40, line 4, "which" is unclear and should be replaced with "wherein the".

aa. Claim 40, line 9, "which" is unclear and should be replaced with "wherein the".

Claim Rejections - 35 USC § 101

11. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

12. Claims 22-35 and 41 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 22-35 and 41 are directed

towards a data structure, which is directed toward nonfunctional descriptive material and is not tangibly embodied.

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 1-7, 12-25, 28-37 and 39-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Muftic and in further view of "Handbook of Applied Cryptography" by Menezes.

Regarding claims 1-2 as best understood, Muftic discloses a method of communication, the method comprising the steps of: a first party/U2 (fig. 4, #430), communicating to a second party/U1 (fig. 4, #450), a composite credential/certificate (fig. 3), across a distributed electronic network/Internet (col. 10, lines 35-37), where in the composite credential/certificate, comprises a plurality of credentials (fig. 3, #300-370), the second party/U1, communicates at least part of the composite credential/certificate, to a third party/CA3 (fig. 4, #420). Muftic fails to explicitly teach that a certificate can be communicated from a CA as well as the user. However, Menezes teaches a certificate may come from a user/trusted third party, (page 39, §1.11.3). One of ordinary skill in the art would have been motivated to modify the method of Muftic with the method of Menezes to allow a certificate to come from a user because a trusted third party may have access to the secret or private keys of users

and therefore send a certificate. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Muftic with the method of Menezes.

Regarding claims 3-4 as best understood and modified above, Muftic further discloses the second party/U1, receives a composite credential/certificate, and the second party/U1, modifies/encrypts, the received composite credential/certificate, before communicating it to the third party/CA3, (col. 12, lines 49-51), in which the second party/U1, receives a composite credential/certificate, and the second party/U1, communicates the received composite credential/certificate, to the third party/CA3, (fig. 4).

Regarding claims 5-7 as best understood and modified above, Muftic further discloses at least one credential in the composite credential/certificate, is obfuscated/encrypted, in which a plurality of credentials in the composite credential/certificate, is obfuscated/encrypted, in which all credentials are obfuscated/encrypted, within the composite credential/certificate.

Regarding claim 12 as best understood and as modified above, Muftic further discloses the composite credential/certificate, comprises a first credential and a second credential in which the second credential is enveloped by the first credential/digest (col. 12, lines 54-56).

Regarding claims 13-14 as best understood and as modified above, Muftic further discloses a first party/U2, communicates to a second party/U1, an obfuscated/encrypted, composite credential/certificate, comprising a first credential and

a second credential in which the second credential is enveloped by the first credential/digest, which obfuscated/encrypted, composite credential/certificate, is de-obfuscated/decrypted, by the second party/U1, thereby to obtain the first credential and a partly de-obfuscated/decrypted, second credential, which partly de-obfuscated/decrypted, second credential is communicated by the second party/U1, to a third party/CA3, in which the third party/CA3, de-obfuscates/decrypts, the partly de-obfuscated/decrypted, second credential, (col. 12, lines 56-60).

Regarding claims 15-16 as best understood and as modified above, Muftic further discloses the composite credential/certificate, is obfuscated/encrypted, in which the first party/U2, communicates to the second party/U1, the composite credential/certificate, (Fig. 4), which composite credential/certificate, is at least partly obfuscated/encrypted, and the second party de-obfuscates/decrypts a relevant credential (fig. 5, #530 or #510).

Regarding claims 17-20 as best understood and as modified above, Muftic further discloses at least one credential is digitally signed, in which a plurality of credentials is digitally signed, in which all credentials in the composite credential/certificate, are digitally signed, in which the composite credential/certificate, is digitally signed (col. 11, lines 36-38).

Regarding claim 21 as best understood and as modified above, Muftic further discloses the distributed electronic network is the Internet (col. 10, lines 35-37).

Regarding claim 28, Muftic further discloses a composite credential according to claim 23, in which the obfuscation comprises asymmetric encryption (col. 11, lines 48-53).

As per claims 22-25, 29-37 and 39-41 as best understood, are rejected under similar rational as discussed above, wherein all claimed limitations have also been addressed and/or cited as set forth above.

15. Claims 8-11, 26-27 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 5,745,574 to Muftic as applied to claims 1-7, 12-25, 28-37, and 39-41 and further in view of U.S. Patent Number 5,497,421 to Kaufman et al. (Kaufman).

Regarding claims 8-10 as best understood, Muftic lacks using different obfuscation for a plurality of credentials. Kaufman teaches a method of communication according to claim 6, in which different obfuscation/double encryption, is used for at least two credentials in the composite credential/certificate, and in which different obfuscation/double encryption, is used for each obfuscated credential in the composite credential/certificate, (col. 9, lines 30-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Muftic with the method of Kaufman. One of ordinary skill in the art would have been motivated to perform such a modification because Kaufman teaches using different double encryption for each separate credential is more secure than encrypting a set of credentials as a whole.

Regarding claim 11 as best understood, Muftic further discloses a method of communication according to claim 8 as modified above, in which the plurality of credentials are obfuscated/encrypted, the second party/U1, de-obfuscates/decrypts (fig. 5, #530 or #510), at least one credential (col. 12, lines 51-52), and communicates to a third party at least one obfuscated credential from the composite credential (col. 13, lines 13-16).

As per claims 26-27 and 38 as best understood, are rejected under similar rational as discussed above, wherein all claimed limitations have also been addressed and/or cited as set forth above.

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

bb. U.S. Patent Number 5,757,920 to Misra et al. is cited for encrypting a digitally signed and sealed certificate of credentials.

cc. U.S. Patent Number 5,497,422 to Tysen et al. is cited for teaching a digitally signed message protected with a chain of encrypted certificates comprising a plurality of credentials.

dd. U.S. Patent Number 6,131,090 to Basso, Jr. et al. is cited for communicating a composite credential to a third party for verification.

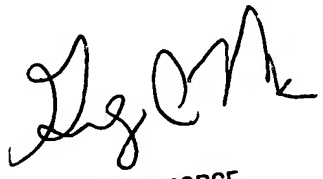
ee. U.S. Patent Application Number 2002/0138728 to Parfenov et al. is cited for encrypting credentials into separate messages.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Berger whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, 7:30 a.m. - 5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Greg Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AHB



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100